IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEIZURE OF:	)	Case No. 1-22-sw-596
	)	
THE DOMAIN NAMES	)	**Filed Under Seal**
simexcbr.com, simexlua.com, simexwim.com,	)	
simexarts.com, simexrue.com, simexvtn.com and	)	
simexbiz.com	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Chris Saunders, being duly sworn, hereby declare as follows:

INTRODUCTION

1. I am a Special Agent with the United States Secret Service ("USSS"). I have been employed by the USSS since December 30, 2018. I am thus a "federal law enforcement officer" as defined by Fed. R. Crim. P. 41(a)(2)(C). I am currently assigned to the Global Investigative Operation Centers ("GIOC") at the Criminal Investigative Division ("CID") located at USSS Headquarters. I have received specialized training in the area of cryptocurrency crimes. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Glynco, Georgia and the USSS Special Agent Training Course in Beltsville, Maryland. I am a Certified Public Accountant and my duties include conducting criminal investigations into complex financial crimes, cryptocurrency crimes, computer fraud, access device fraud, wire fraud, mail fraud, identity theft, telecommunications fraud and money

laundering. In these investigations, I have been involved in the execution of warrants.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. As set forth below, there is probable cause to believe that the **SUBJECT DOMAIN NAMES**, **simexcbr.com, simexlua.com, simexwim.com, simexarts.com, simexrue.com, simexvtn.com and simexbiz.com** are involved in violations of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering).**(**SUBJECT OFFENSE), and subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1). I make this affidavit for a warrant to seize the property described in Attachment A, specifically, the **SUBJECT DOMAIN NAMES**.

4. The procedure by which the government will seize the Domain Name is described in Attachment A hereto and below.

BACKGROUND ON DOMAIN NAMES

5. Based on my training and experience and information learned from others, I am aware of the following:

6. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers,

each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

7. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

8. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

9. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses. .For example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

10. Registry: For each top-level domain (such as ".com"), there is a single company,

called a "registry," that determines which second-level domain resolves to which IP address.

11. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services. For example PublicDomainRegistry.com is a registrar located Tempe, Arizona.

12. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

13. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal.

Background of Cryptocurrency

14. Based on my training, research, education, and experience, I am familiar with the

following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[1] Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

b. Bitcoin[3] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not

[1] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[3] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

c. Tether ("USDT") and USD Coin ("USDC") are alternative types of cryptocurrency or altcoin token. Payments or transfers of value made with Tether and USD Coin are recorded in the blockchain network, but unlike decentralized Cryptocurrencies like bitcoin, tether has some anatomical features of

centralization. One centralized feature is that Tether and USD Coin is a Stablecoin or a fiat- collateralized token that is backed by fiat currencies, or currencies issued by governments like the dollar and euro. Tether and USD Coin are backed with a matching one to one fiat amount, making it much less violate than its counterpart, Bitcoin. Due to tether's and USD coins' stable nature, wallet holders typically use a fundamental strategy to hedge their cryptocurrency holdings into tether to hedge their receipt or earnings value so it not affected by the rest of violate cryptocurrency market.

d. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

e. Although cryptocurrencies such as Bitcoin and have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes

such as money laundering, and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

f. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[4] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets

[4] A QR code is a matrix barcode that is a machine-readable optical label.

can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

g. Cryptocurrency "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and tether. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[5] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise

[5] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

h. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different

digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

CASE BACKGROUND

A. Background on spoofed SIMEX domains

15. Between July and September, 2022, the USSS was contacted by a victim in Redmond, WA (herein referred to as "Victim 1"), Los Angeles, CA (herein referred to as "Victim 2"), Columbus, OH (herein referred to as "Victim 3"), Seattle, WA (herein referred to as "Victim 4"), and Richmond, VA (herein referred to as "Victim 5") collectively referred to as "Spoofed Victims" who reported a cryptocurrency investment scam involving numerous spoofed domains of Singapore International Monetary Exchange ("SIMEX") which uses the legitimate domain name sgx.com. Each of the Spoofed Victims were provided a different spoofed domain version of SIMEX. Victim 1 was provided **simexlua.com** and **simexwim.com**; Victim 2 was provided **simexcbr.com**; Victim 3 was provided **simexrue.com** and **simexvtn.com**; Victim 4 was provided**simexarts.com**; and Victim 5 was provided **simexbiz.com**, collectively referred to as **SUBJECT DOMAIN NAMES**. The Spoofed Victims invested cryptocurrency into the **SUBJECT DOMAIN NAMES** trading platforms promoted by unknown scammer(s) (herein referred to as "Suspect 1") and after numerous attempts to withdrawal their investments, they were unable to recover any portion of their cryptocurrency investment.

B. Background on Victim 1

16. In August 2022, the USSS was contacted by Victim 1 who reported a cryptocurrency investment scam. Victim 1 stated they communicated with Suspect 1 on LINE

and WeChat[6] and discussed trading crypto futures. Suspect 1 promoted a cryptocurrency investment platform to Victim 1 and provided the domain URL **simexlua.com,** which is a spoofed version of the SIMEX domain.

17. In May 2022, at the direction of Suspect 1, Victim 1 made an online account at **simexlua.com** utilizing her phone number. Upon logging into their online account, Victim 1 was provided deposit address 0xdd3eda895e7ae66537a1585f1807074a7f7a6eb8 ("0xdd3") through the trading platform at **simexlua.com** for making investments. See figure 1. Suspect 1 then convinced Victim 1 to download the mobile application domain **simexwim.com** and upload their official driver's license for verification purposes.

18. Victim 1 was led to believe that investments to deposit address 0xdd3 would be legitimate investments made to SIMEX. Initially, on or about May 17, 2022, Victim 1 made a small investment of approximately $400 in USD Coin ("USDC"), a type of cryptocurrency. Victim 1 eventually invested approximately $9,600,000.00 (9.6 Million USD) over the course of four months (May, 2022 through August, 2022) from their Coinbase and Bistamp[7] account. Refer to the transactions below obtained from records provided by the Victim 1 and verified on the blockchain.

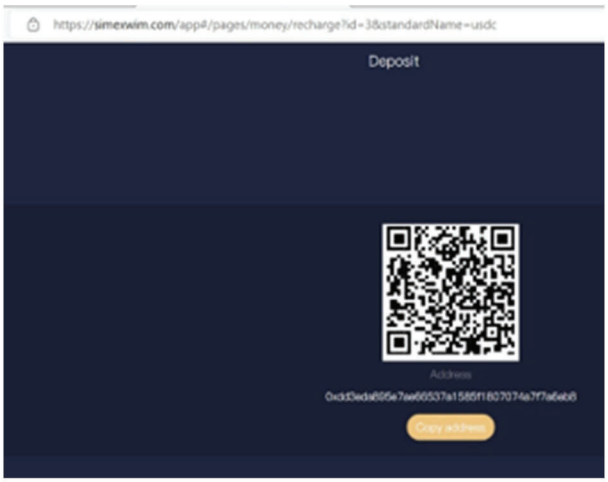
[6] LINE and WeChat are mobile messenger applications based out of Japan and China respectively.

[7] Coinbase and Bitstamp are online exchanges used for buying, selling, trading, and storing cryptocurrency. Both Coinbase and Bitstamp exchanges are legally permitted and licensed to operate in the United States.

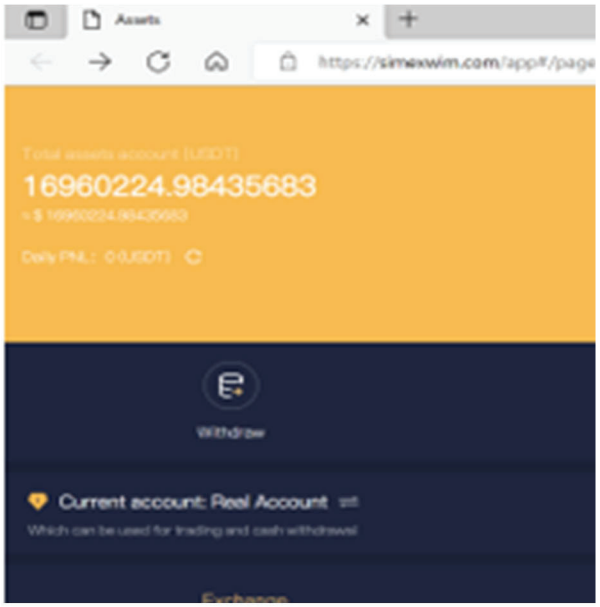
Date	Address	Counterparties	Asset	Amount	Amount USD
2022-08-16 01:44:33.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	100,000.00	$ 100,191.14
2022-08-09 00:58:20.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	162,000.00	$ 162,218.23
2022-08-03 01:01:26.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	528,000.00	$ 528,207.91
2022-07-30 01:46:41.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	360,000.00	$ 359,993.20
2022-07-23 00:55:21.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	200,000.00	$ 200,114.95
2022-07-21 05:41:33.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	495,000.00	$ 495,025.04
2022-07-14 01:07:56.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	490,000.00	$ 489,468.40
2022-07-09 08:10:56.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	70,000.00	$ 70,192.30
2022-07-08 02:38:54.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	411,000.00	$ 411,551.39
2022-07-07 06:25:11.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	47,012.00	$ 47,188.56
2022-07-06 01:11:34.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	450,000.00	$ 451,230.58
2022-07-06 01:11:34.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	383,037.53	$ 384,084.99
2022-06-28 00:40:35.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	480,000.00	$ 480,309.11
2022-06-24 01:16:46.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	452,000.00	$ 453,518.99
2022-06-24 00:45:47.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	450,000.00	$ 451,512.27
2022-06-18 07:56:07.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	370,500.00	$ 371,530.51
2022-06-18 07:56:07.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	400,000.00	$ 401,112.56
2022-06-18 07:56:07.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	366,000.00	$ 367,017.99
2022-06-14 02:11:36.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	357,326.41	$ 357,395.21
2022-06-14 02:11:33.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	300,000.00	$ 300,057.77
2022-06-14 01:42:26.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	300,000.00	$ 300,057.77
2022-06-08 07:13:03.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	323,567.65	$ 323,421.84
2022-06-08 07:13:03.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	390,000.00	$ 389,824.25
2022-06-08 06:46:01.000Z	0x1522900b6dafac587d499a862861c0869be6e428	Bitstamp	USDC	400,000.00	$ 399,819.75
2022-05-26 19:57:50.000Z	0x3cd751e6b0078be393132286c442345e5dc49699	Coinbase	ETH	320.98	$ 589,383.28
2022-05-25 19:24:30.000Z	0xb5d85cbf7cb3ee0d56b3bb207d5fc4b82f43f511	Coinbase	ETH	159.48	$ 313,609.58
2022-05-23 23:28:44.000Z	0xb5d85cbf7cb3ee0d56b3bb207d5fc4b82f43f511	Coinbase	ETH	149.49	$ 299,250.07
2022-05-20 23:30:23.000Z	0x503828976d22510aad0201ac7ec88293211d23da	Coinbase	USDC	100,462.25	$ 100,581.02
2022-05-17 01:05:03.000Z	0x503828976d22510aad0201ac7ec88293211d23da	Coinbase	USDC	381.37	$ 382.44

19. During an interview on August 23, 2022, Victim 1 provided agents with numerous screen shots from their **simexlua.com** desktop platform and **simexwim.com** mobile application account profile noting instances of "trading profit" after each investment transaction. For example, on July 25, 2022, Victim 1 received a "trading profit" transaction of USDC 2,832,200 which was added to their account. Victim 1 stated that their account on **simexlua.com** led her to believe she had earned over $7,000,000 in profit. See figure 1 for examples of fictitious profit on Victim 1's account at **simexlua.com** and **simexwim.com.**

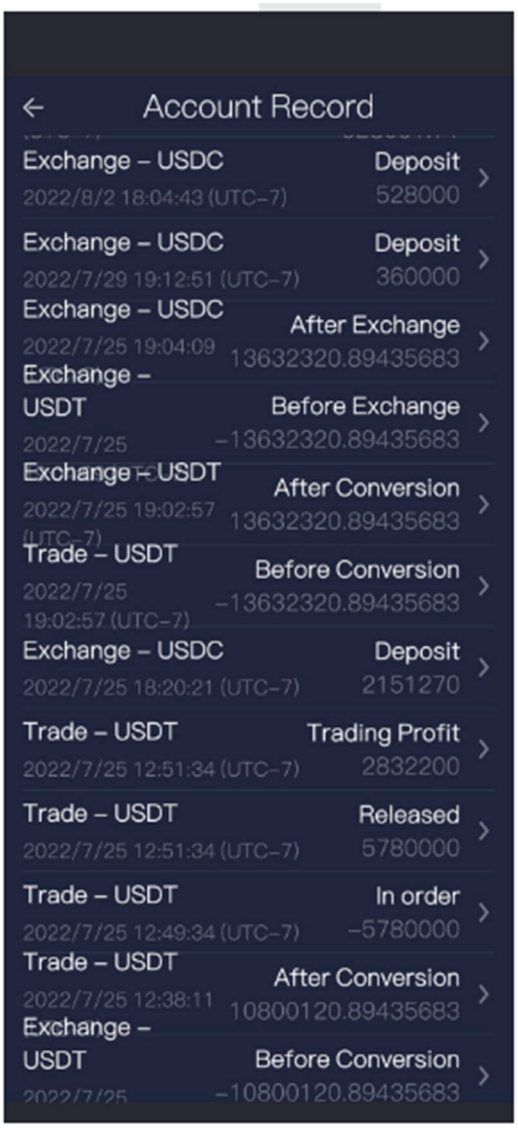
Figure 1.



Deposit address provided by simexlua.com



Account balance with pofitt shown on simexlua.com



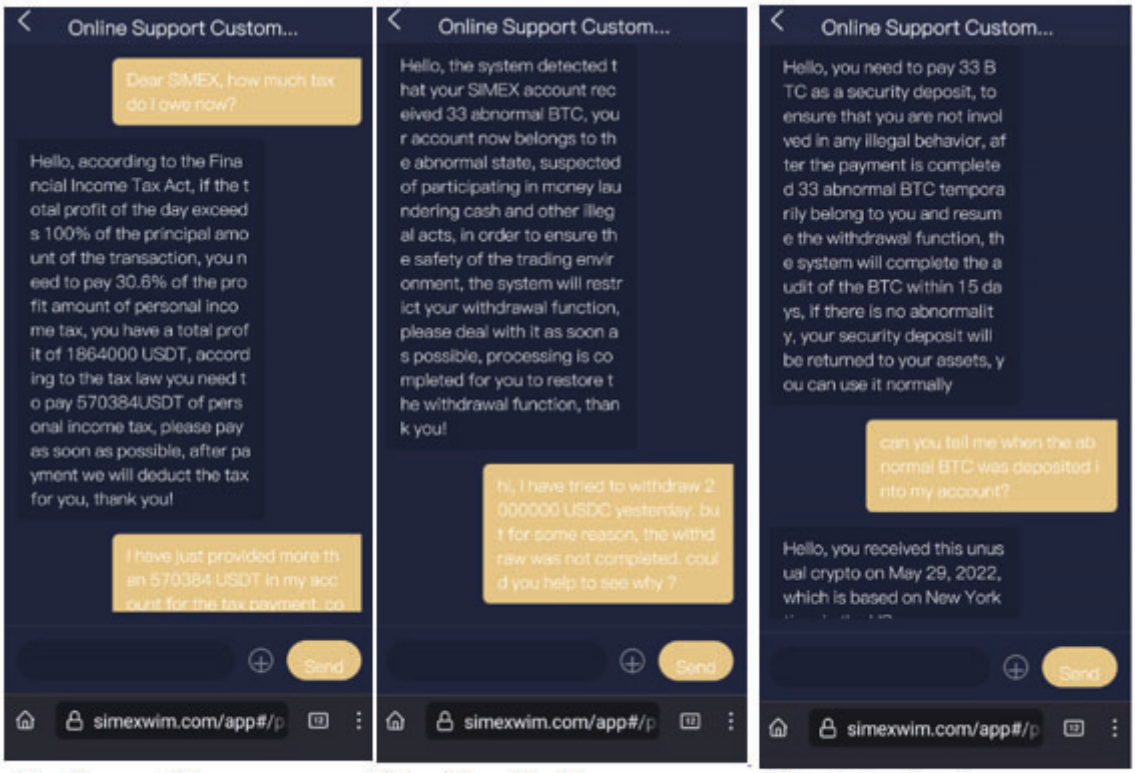
Daily trading profit from simexwin.com

20. Victim 1 informed law enforcement that each time they attempted to make withdrawals from their accounts, they received requests from **simexlua.com** and **simexwim.com's** customer service representatives asking them to make additional payments in the form of "taxes" or "fees" in order to regain access to their account. For example, on May 23, 2022, the customer service chat platform on **simexwim.com** informed Victim 1 "*according to Financial Income Tax Act, if the total profit of the day exceeds 100% of the principal amount of*

the transaction, you need to pay 30.6% of the profit amount of personal income tax, you have a total profit of 1864000 USDT, according to the tax law you need to pay 570384USDT of personal income tax, please pay as soon as possible, after payment we will deduct the tax for you, thank you!". Between May 23 and May 25, 2022, Victim 1 transferred USDC from their Coinbase account to deposit address 0xdd3 in order to make the "income tax payments". Refer to figure 2 for examples of messages from the customer service online chat platform at simexwim.com.

21. In June 2022, Victim 1 attempted to make additional withdrawals, and **simexwim.com** online customer support noted "*...the system detected that your SIMEX account received 33 abnormal BTC, your account now belongs to the abnormal state..." and "you need to pay 33 BTC as a security deposit, to ensure that you are not involved in any illegal behavior...".* Refer to figure 2 below. This tactic of Suspect 1 and customer service requesting "taxes" and "fees" continued until August when Victim 1 determined it was a scam and stopped making investments.

Figure 2



C. Spoofed SIMEX Domains Undercover Activities

22. As part of their investigation, on or around September 1, 2022, case agents conducted an undercover operation ("UCO") in which an undercover agent ("UCA") visited the spoofed domains and created an account at **simexlua.com.** While creating an account, the UCA was instructed by the website to provide either an email address or phone number. The UCA received a verification email from simex.radmails.com with a one-time verification code. Further investigation reveals that radmails.com domain is connected to the **SUSPECT DOMAIN NAMES** through similar registrant information such as name, phone number and organization. Upon successfully creating an account, the UCA navigated to the trading platform to execute a deposit and was provided with deposit addresses for a number of different cryptocurrencies including USDT, USDC, ETH and BTC. The undercover action also revealed that the UCA

account login information at **simexlua.com** worked for each of the other **SUSPECT DOMAIN NAMES**. The UCA account information such as name, phone number and email address carried over to each of the **SUSPECT DOMAIN NAMES**. In addition, the deposit address provided to the UCA in order to make investments is the same for each of the **SUSPECT DOMAIN NAMES**.

23. Additionally, on or about September 1, 2022, the UCA reviewed the webpages of the **SUBJECT DOMAIN NAMES** noting each of the websites were identical. See figure 3 for screen shot examples of the **SUBJECT DOMAIN NAMES**. The **SUBJECT DOMAIN NAMES** contained similar trademark, copywrite and about page details which were clearly taken from the legitimate SIMEX domain sgx.com. For example, the about page of sgx.com notes that in 1984 "*Singapore International Monetary Exchange (SIMEX) was founded as the first financial futures exchange in Asia*" and the **SUBJECT DOMAIN NAMES** state "*Singapore International Monetary Exchange (SIMEX) founded in 1984, is the first financial futures exchange in Asia*". The sgx.com domain about page continues and notes in 1989 "*SIMEX launched Asia's first oil futures contract to try to meet the needs of the domestic fuel oil market*" and the **SUBJECT DOMAIN NAMES** about page notes "*1989, SIMEX became the first energy futures trading market in Asia*".

24. Further investigation revealed that domain whois records for the **SUBJECT DOMAIN NAMES** all contain the same registrant information. Based on my training and experience I know that it is common for cyber criminals spoofing domains to use the same registrar information when mass producing domains. In addition, each of the **SUBJECT DOMAIN NAMES** URL all start with SIMEX and change the last two or three letters.

a. All **SUBJECT DOMAIN NAMES** have common registrar information as

follows:

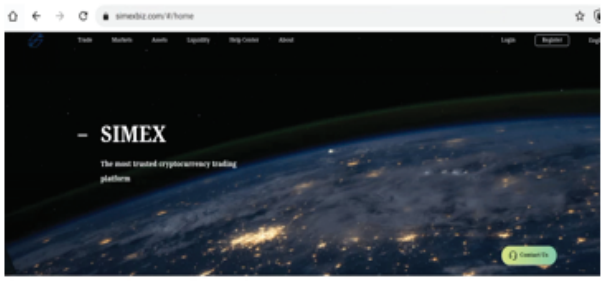
- Registrant Org: main
- Registrant Phone: +852.67308658
- Registrant Street: hongkong 123456
- Registrant Contact Postal: 999077
- Registrant City: hongkong

Figure 3

simexcbr.com

simexarts.com

simexlua.com



simexbiz.com

D. Blockchain Analytics

25. During interviews with the Spoofed Victims, agents learned that each victim of the spoofed SIMEX domains received a different deposit address provided by the spoofed domain.

i) Victim 1: 0xdd3eda895e7ae66537a1585f1807074a7f7a6eb8

ii) Victim 2: 0x105407fce6e6038b1271dd8da6f98e3b02c6f16d

iii) Victim 3: 0x16b47be43b01bd89a97f1b2de7ae2f7616d692b2

iv) Victim 4: 0xd3e1c43ea136a42f8d7f494cec3fc5d9d9cba40c

v) Victim 5: 0x6ab765e54834979f5b2ee890ffcd68f42cf2b18c

26. Using reliable third-party blockchain analytic software[8] and open source blockchain explorers, law enforcement officers reviewed the blockchain and noted these addresses are consistent with "Burner" addresses as these addresses were created solely to receive Victim proceeds and there were no other transactions in these addresses. In addition, the fraud proceeds were immediately withdrawn from these addresses and sent to a common intermediary deposit address 0x308fcb6c4e169b090f42d0968326391d9e53859c ("0x308"). As a result, these subsequent transactions zeroed out the balance in the initial address into which the Victims transferred their investments.

27. It is noted the deposit addresses provided to the Spoofed Victims for investments are private addresses, therefore, the Victims lost control and access to the funds as they did not possess the private keys. Based on my training and experience scammers use "Burner" wallet addresses to quickly transfer funds to multiple private wallets addresses in order to conceal and obfuscate the nature of the proceeds.

[8] Law enforcement uses sophisticated, commercial services offered by several blockchain-analysis companies to investigate bitcoin transactions. These companies analyze the blockchain in an attempt to identify the individuals or groups involved in the bitcoin transactions. Specifically, these companies create large databases that group bitcoin transactions into "clusters" through analysis of data underlying bitcoin transactions. Thus, the service allows law enforcement to utilize third-party blockchain analysis software to locate bitcoin addresses that transact at the same time (i.e., the blockchain logs transactions that occur at the same time by two different bitcoin addresses) and "cluster" these addresses together to represent the same owner. This third-party blockchain analysis software is used by banks and law enforcement worldwide. This third-party blockchain analysis software has supported many investigations and has been the basis for numerous search-and-seizure warrants, and consequently, the intelligence provided has been found to be reliable. Additionally, computer scientists have independently shown that they can use "clustering" methods to take advantage of clues in how bitcoins are typically aggregated or split up to identify bitcoin addresses and their respective account owners.

28. Further blockchain review and investigative efforts reveals the common intermediary address 0x308 is a private wallet address which uses the swapping service Tokenlon[.]im[9] in order to swap Spoofed Victim proceeds from ETH and USDC to USDT before they were transferred to additional addresses. Based on my training and experience, scammers are known to utilize private wallet services like Tokenlon to obfuscate and conceal proceeds by swapping the initial cryptocurrency virtual coin into a different virtual coin (e.g., USDC to USDT). Private wallets are non-custodial wallets, meaning the owner, as opposed to the host, controls the private keys. Private non-custodial wallets can be held in numerous forms such as, wallet applications on computers and cell phones, cold storage devices not connected to the internet, and paper wallets.

29. After being swapped into USDT using TokenIon, the proceeds of both Victim 1 and the Spoofed Victims, were immediately transferred to numerous other addresses. When Spoofed Victims transferred investments into the deposit addresses provided by **SUBJECT DOMAIN NAMES**, their funds were immediately transferred through numerous private wallets and swapping services in an effort to conceal the source of funds.

30. For example, on 6/28/22, Victim 1 transferred 480,000 USDC from their Bitstamp account to the initial address provided by **simexlua.com** and **simexwim.com** (0xdd3eda895e7ae66537a1585f1807074a7f7a6eb8; TXID 0xf8c1f4…). On the same day, Suspect 1 transferred 480,000 USDC to the TokenIon address 0x308 to be swapped into USDT and then immediately transferred the USDT proceeds to address 0xa9c96e5093305e0c22a76d10b112dbb7f4389d83 (TXID 0xeec100…). All of these transfers, including the TokenIon swap occurred within 2 hours. From 0xa9c the proceeds are then

[9] TokenIon[.]im is a decentralized service which allows users to swap virtual currencies.

commingled with other funds and deposited into numerous OKX[10] addresses. Based on my training and experience, I know that criminals make numerous transfers and conduct swaps in a short period of time to conceal and obfuscate the source of proceeds. In addition, based on my training and experience, I know that criminals tend to use exchanges such as OKX because they are not known to collect Know Your Customer (KYC) information or employ Anti-money Laundering policies which are intended to stop criminals from disguising fraudulent proceeds.

E. Victim 2

31. On August 10, 2022, Victim 2 transferred 204,575 USDC from their Cyrpto.com[11] account to the deposit address provided by **simexcbr.com** (0x105407fce6e6038b1271dd8da6f98e3b02c6f16d; TXID: 0x0cec8e…). On the same day, Suspect 1 transferred 204,575 USDC to the TokenIon address 0x308 to be swapped into USDT and then immediately transferred the USDT proceeds to address 0x3a5d037f8e5ffd692a8a789cfc464a8313c2db23 (TXID: 0x8d1ff1…). From the 0x3a5 address the proceeds are then commingled and deposited into numerous OKX addresses.

F. Victim 3

32. On August 20, 2022, Victim 3 transferred 99,990 USDC from their Cyrpto.com account to the deposit address provided by both **simexvtn.com** and **simexrue.com** (0x16b47be43b01bd89a97f1b2de7ae2f7616d692b2; TXID: 0xb181be…). On the same day, Suspect 1 transferred 99,990 USDC to the TokenIon address 0x308 to be swapped into USDT and then immediately transferred the USDT proceeds to address

[10] OKX is a cryptocurrency exchange which is based in the Republic of Seychelles and is not available for use in the U.S. due to regulatory and compliance reasons.

[11] Crypto.com is an online exchange used for buying, selling, trading, and storing cryptocurrency. Crypto.com is legally permitted and licensed to operate in the United States.

0x3a5d037f8e5ffd692a8a789cfc464a8313c2db23 (TXID 0x587b6f…). From the 0x3a5 address the proceeds are then commingled and deposited into numerous OKX addresses.

G. Victim 4

33. On July 20, 2022, Victim 4 transferred 50,986.74 USDC from her Coinbase account to the deposit address provided by **simexarts.com** (0xd3e1c43ea136a42f8d7f494cec3fc5d9d9cba40c; TXID: 0x0cec8e…). On the same day, Suspect 1 transferred 50,986.74 USDC to the TokenIon address 0x308 to be swapped into USDT and then immediately transferred the USDT proceeds to address 0x3a5d037f8e5ffd692a8a789cfc464a8313c2db23 (TXID 0x5478d5…). From the 0x3a5 address the proceeds are then commingled and deposited into numerous OKX addresses.

H. Victim 5

34. On July 20, 2022, Victim 5 transferred 289,065.15 USDC from their Bitstamp account to the deposit address provided by simexbiz.com, 0xd3e1c43ea136a42f8d7f494cec3fc5d9d9cba40c (TXID: 0x0cec8e…). On the same day, Suspect 1 transferred 289,065.15 USDC to the TokenIon address 0x308 to be swapped into USDT and then immediately transferred the USDT proceeds to address 0x86f3f09c0b47b0697581f963b2955ac63ddbe656 (TXID 0xa80407…). . From the 0x86f address the proceeds are then commingled and deposited into numerous OKX addresses.

THE SUBJECT DOMAIN NAME

35. As described above, the **SUBJECT DOMAIN NAMES** were involved in concealment money laundering.

36. A search of publicly available WHOIS domain name registration records revealed that the **SUBJECT DOMAIN NAMES** were registered during May, June and July through the

registrar PDR Ltd. d/b/a PublicDomainRegistry.com, which has is located in Tempe, Arizona.

37. Because the **SUBJECT DOMAIN NAMES** were purchased through PublicDomainRegistry.com, which acts as the intermediary between the registry and the purchasers of the **SUBJECT DOMAIN NAMES,** PublicDomainRegistry.com is the registrar

38. Because Verisign manages all .com and .net domains, the top-level domain for the **SUBJECT DOMAIN NAME** is Verisign.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

39. Title 18, United States Code, Section 981(a)(1)(A) provides, in relevant part, that any property involved in a transaction or attempted transaction in violation of the prohibition of Title 18, United States Code, Sections 1956 and 1957 is subject to civil forfeiture to the United States government.

40. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

41. Title 18, United States Code, Section 982(a)(1) provides, in relevant part, that any property involved in a transaction or attempted transaction in violation of Title 18, Untied States Code Sections 1956 and 1957 is subject to criminal forfeiture to the United States government.

42. Title 18, United States Code, Section 982(b)(1) authorizes the issuance of a criminal seizure warrant under Title 21, United States Code, Section 853(f) which provides in relevant part that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant

if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

43. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT DOMAIN NAMES** for forfeiture. By seizing the **SUBJECT DOMAIN NAMES** and redirecting it to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the **SUBJECT DOMAIN NAMES** will prevent third parties from continuing to access the **SUBJECT DOMAIN NAME**S in its present form.

44. Title 18, United States Code, Section 981(h) provides that venue for civil forfeitures brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought. Section 981(h) applies only in cases of property of a defendant charged with a violation that is the basis for the forfeiture of the property. Otherwise, under section 981(h), venue is determined under Title 28, United States Code, Section 1395. Section 1395 provides that a civil forfeiture action may be maintained in the district where the offense giving rise to forfeiture was committed, the district where the subject property is found, or any district into which the property is brought.

45. As set forth above, there is probable cause to believe that the **SUBJECT DOMAIN NAMES** are subject to civil and criminal forfeiture because they were used in the commission of violations of the SUBJECT OFFENSE. Specifically, the **SUBJECT DOMAIN NAMES** were involved in – and enabled –the individuals controlling these domain addresses to launder the proceeds of a specified unlawful activity and engage in monetary transactions in property derived from a specified unlawful activity in violation of the SUBJECT OFFENSE.

SEIZURE PROCEDURE

46. As detailed in Attachment A, upon execution of the seizure warrant, the registrar for the .com top-level domain, VeriSign, headquartered at 12061 Bluemont Way, Reston, VA 20190, shall be directed to restrain and lock the **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the United States Secret Service or the Department of Justice.

47. In addition, upon seizure of the **SUBJECT DOMAIN NAMES** by the United States Secret Service, VeriSign will be directed to associate the **SUBJECT DOMAIN NAMES** to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the **SUBJECT DOMAIN NAMES** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

48. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAMES** is used in and/or intended to be used in facilitating and/or committing the SUBJECT OFFENSE. Accordingly, the **SUBJECT DOMAIN NAMES** are subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1), and I respectfully request that the Court issue a seizure warrant for **SUBJECT DOMAIN NAMES**.

49. Because the warrant will be served on VeriSign, which controls the **SUBJECT DOMAIN NAMES**, and VeriSign, thereafter, at a time convenient to it, will transfer control of the **SUBJECT DOMAIN NAMES** to the government, there exists reasonable cause to permit

the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Christopher Saunders

Christopher Saunders
Special Agent
United States Secret Service

Subscribed and sworn to in accordance with Fed. R. Crim. Proc. 4.1
by telephone on November 16, 2022

William E. Fitzpatrick

The Honorable William E. Fitzpatrick
United States Magistrate Judge

ATTACHMENT A

With respect to **simexcbr.com, simexlua.com, simexwim.com, simexarts.com, simexrue.com, simexvtn.com and simexbiz.com** ("**SUBJECT DOMAIN NAMES**"), VeriSign, who is the domain registry for the **SUBJECT DOMAIN NAMES**, shall take the following actions to effectuate the seizure of **SUBJECT DOMAIN NAMES**:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the United States Secrete Service, by modifying the **SUBJECT DOMAIN NAMES** authoritative DNS server entries to include the following:

   a) ns1.usssdomainseizure.com

   b) ns2.usssdomainseizure.com

   or:

   Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to VeriSign.

2) Prevent any further modification to, or transfer of, **SUBJECT DOMAIN NAMES** pending transfer of all right, title, and interest in **SUBJECT DOMAIN NAMES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **SUBJECT DOMAIN NAMES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Secret Service.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

5) The Government will display a notice on the website to which the **SUBJECT DOMAIN NAMES** will resolve. That notice will consist of law enforcement emblems and the

following text (or substantially similar text):

"The domain for each of the **SUBJECT DOMAIN NAMES** has been seized pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Virginia in accordance with 18 U.S.C. §§ 981 and 982, as part of law enforcement action by:

- US Department of Justice – Eastern District of Virginia
- United States Secret Service – Washington D.C. Criminal Investigative Division
- US Department of Justice - National Cryptocurrency Enforcement Team